

ABSTRACT OF THE INVENTION

A system and methods of enhancing a server's ability to withstand a SYN flood type denial of service attack are presented. Modifications to the TCP/IP layer of a server reduce the amount of system resources that are allocated, and the amount of CPU overhead that is required to process a connection request until the TCP/IP three-way handshake is completed to verify the presence of a legitimate client. Specifically, the TCP/IP layer allocates a small TCP control block (TCB) of a size sufficient only to service the connect request upon receipt of the SYN packet. A full TCB is not allocated until the connection is completed. Further, the TCP/IP layer delays notification to the socket layer of the receipt of the SYN packet until after the connection is completed. Finally, the route information of the connection is not cached until after the connection is completed. These methods, individually, or in combination, significantly enhance a server's ability to withstand a SYN flood attack.